May 1993

Risk Assessment Methodology for EDI Unclassified/Sensitive Information Systems

DL203R3

Julie A. Smith

Prepared pursuant to Department of Defense Contract MDA903-90-C-0006. The views expressed here are those of the Logistics Management Institute at the time of issue but not necessarily those of the Department of Defense.

Logistics Management Institute
6400 Goldsboro Road
Bethesda, Maryland 20817-5886

Executive Summary

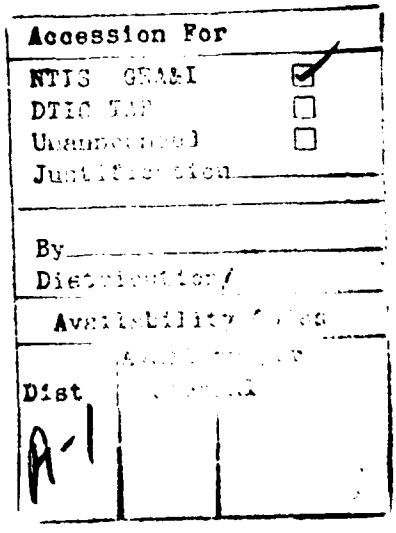
RISK ASSESSMENT METHODOLOGY FOR EDI UNCLASSIFIED/SENSITIVE INFORMATION SYSTEMS

The Computer Security Act of 1987, DoD Directive 5200.28 entitled *Security Requirements for Automated Information Systems* (dated 21 March 1988), and various other Government regulations stress the importance of maintaining an awareness of the level of risk inherent within the implementation of appropriate information security procedures for information systems. Because it is not cost-effective to implement more security procedures than a particular environment requires, defining security requirements based on the results of a thorough risk analysis provides an effective way to control the cost of security for information systems. Early in their planning process, individuals overseeing DoD's program for Electronic Commerce (EC) and electronic data interchange (EDI) recognized that it required special techniques to analyze the unique information security problems posed by EDI. As a result, the Logistics Management Institute (LMI) developed an EDI risk assessment methodology.

An important goal in developing a risk assessment methodology is to design a guideline that is easy to use, but that also provides a somewhat structured format for documenting security requirements and how they are being met. Given that EDI security technology is still evolving, LMI's methodology provides the decision maker with a high degree of latitude in selecting information protection that best suits his/her environment. LMI's methodology recommends the use of self-assessment worksheets to identify security requirements.

The steps involved in the EDI risk assessment methodology are the same basic steps found in most types of risk assessment: define assets, review threats, identify security requirements, and select protective countermeasures. The methodology addresses all of the primary threats to an EDI application system and its data, which include the following: unauthorized disclosure of data, unauthorized modification of data, sender repudiation of transactions, receiver repudiation of transactions, unauthorized system access, and lack of system availability. The methodology is

structured so that each module builds on the previous one. Additionally, one module requires users to identify the information flow in their EDI business process by listing the types of actions that will be automated using EDI. The users are then asked to determine whether or not sensitive data are being processed for each type of action, and, if the data are sensitive, to identify the type of sensitive data. The methodology emphasizes defining terminology related to EDI security since many of the users of the methodology have had little prior exposure to working with EDI security. The methodology also stresses that it is very important to involve a designated information systems security professional in the EDI risk assessment process.



CONTENTS

	Page
Executive Summary	ii
Chapter 1. Introduction	1
Chapter 2. Define Assets and Inventory Software	5
Worksheet 1 – *Define Assets*	6
Worksheet 2 – *Inventory Software*	7
Chapter 3. Determine Data Sensitivity	8
Document the Information Flow	8
Define the Type of Sensitive Data	8
Worksheet 3 – *Sensitivity of EDI Data*	11
Chapter 4. Review Threats and Identify Information Security Requirements	13
Overview	13
General Instructions for Worksheets 4.1 and 4.2	13
Worksheet 4.1 – *System-Wide Information Security Requirements*	17
Worksheet 4.2 – *Action-Specific Information Security Requirements*	21
Chapter 5. Select Protective Countermeasures	22
Worksheet 5.1 – *Countermeasures Identification, System-Wide Information Security Requirements*	25
Worksheet 5.2 – *Countermeasures Identification, Action-Specific Information Security Requirements*	26
Glossary	27

CHAPTER 1

INTRODUCTION

The Computer Security Act of 1987 defines *sensitive information* as follows:

> Any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under . . . the Privacy Act, but which has not been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.

Based on this definition, some examples of sensitive information are as follows:

- Vital records
- Privacy Act information
- Official use only information
- National security-related (but unclassified) information
- Security management information
- Proprietary information.

Electronic data interchange (EDI) transactions that involve the transfer of any unclassified/sensitive information should employ some level of protection if the EDI data are to be transmitted safely.

The purpose of this risk assessment methodology is to enable organizations to determine where their information security vulnerabilities lie with respect to the use of an information system for the EDI of unclassified/sensitive information. Organizations should use the information obtained about vulnerabilities to allocate information security resources for protection of EDI data commensurate with the level of risk involved. A risk assessment should be performed for each unique information system architecture that performs EDI transactions.

Both Department of Defense Directive (DoDD) 5200.28 (dated 21 March 1988) and the Computer Security Act of 1987 discuss the importance of maintaining an awareness of the level of risk to which sensitive but unclassified data are exposed

within systems. Owners of DoD systems are required by DoDD 5200.28 to conduct a complete information security risk assessment for each information system that processes sensitive but unclassified information and also to maintain a risk management program for each system. Because the risk assessment methodology presented in this report focuses on the EDI application system, it is meant to function as an addition to the overall information system security risk assessment, not as a replacement for that total assessment.

It is important to involve a qualified information systems security professional in the EDI application system risk assessment process from the beginning to ensure that proposed security mechanisms are technically feasible and implemented correctly, and that the cost of data protection is consistent with the level of risk to which those data are exposed.

This risk assessment methodology has the following four main parts:

- *Chapter 2* – define assets by describing the system used to perform EDI transactions.
- *Chapter 3* – determine the sensitivity of the data to be exchanged in the EDI system.
- *Chapter 4* – assess whether or not basic areas of vulnerability are protected.
- *Chapter 5* – review and select information security mechanisms that would ensure that the data in EDI transactions are or will be protected commensurate with the level of risk to the system.

Sections of this risk assessment methodology are adapted from the *U.S. Department of Energy (DOE) Risk Assessment Methodology, Volumes I and II*, issued by the U.S. Department of Commerce, National Technical Information Service in May 1990. The EDI security concepts addressed are based on a Computer Systems Laboratory (CSL) Bulletin entitled *Security Issues in the Use of Electronic Data Interchange* issued by the National Institute of Standards and Technology (NIST) in June 1991.

Read through all instructions provided in Chapters 2 through 5 and examine all worksheets and tables before completing any part of the risk assessment methodology. Figure 1 diagrams the paperwork associated with the assessment process. Figure 2 shows an example of a finished risk assessment.

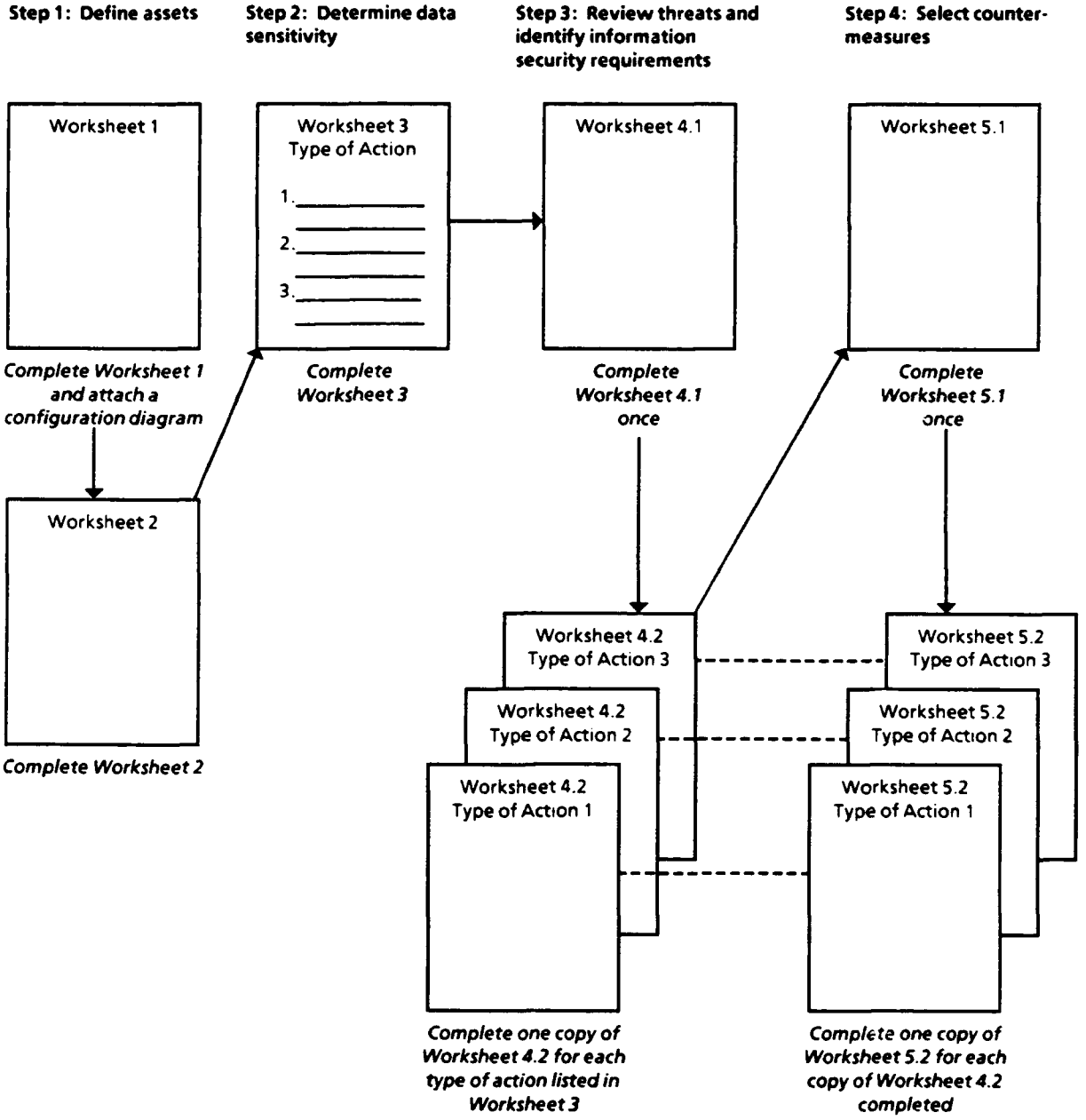


FIG. 1. FLOWCHART OF THE RISK ASSESSMENT METHODOLOGY

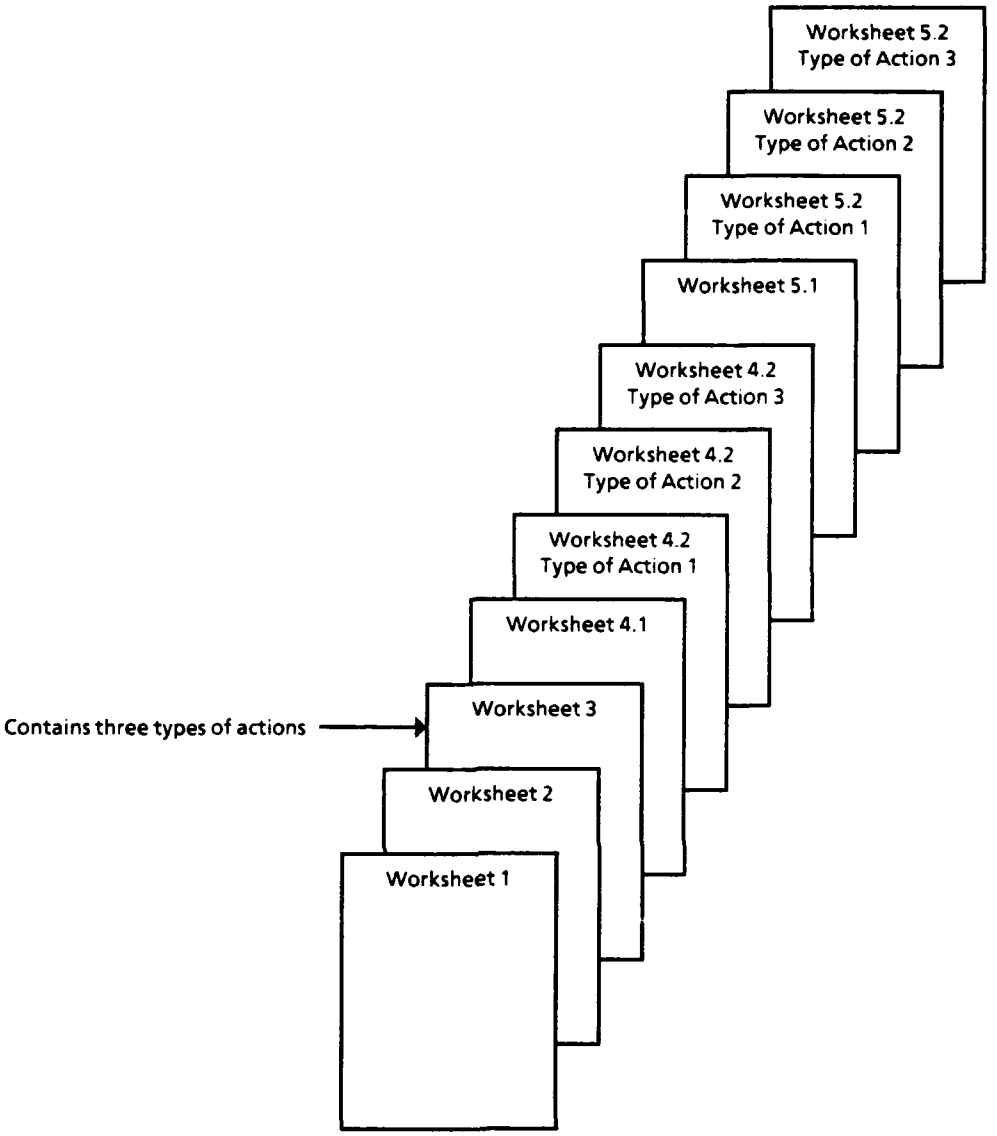


FIG. 2. EXAMPLE OF A COMPLETED RISK ASSESSMENT

CHAPTER 2

DEFINE ASSETS AND INVENTORY SOFTWARE

Assets are defined within the methodology by performing the following steps:

- Provide basic information about the application system that is used for EDI by completing Worksheet 1.
- Attach a configuration diagram to Worksheet 1 that depicts the hardware that is or will be used for EDI and the connections made between machines.
- List, on Worksheet 2, the name(s) of the operating system(s) and application software that are used to perform EDI transactions.

Worksheet 1

Define Assets

1. Provide the following background information about the system that is being assessed:

   System name:

   Organization:

   Location:

   Point of contact:

   Phone: Date:

2. What is or will be the frequency of use of the system? (Check one answer.)

   _____ Periodic (very low): Occasional use during the month

   _____ Monthly (low): Regular use during the month

   _____ Weekly (medium): Regular use during the week

   _____ Daily (high): Regular use during the workday

   _____ Continuous (very high): Continuous use during the workday or use around-the-clock

3. What is or will be the impact upon the organization if the system is unavailable? (Check one answer.)

   _____ Routine (very low): No impact on organization/capability

   _____ Moderately important (low): One month until impact on organization/capability

   _____ Important (medium): One week until impact on organization/capability

   _____ Highly important (high): Two days until impact on organization/capability

   _____ Vital (very high): Immediate impact on organization/capability

Worksheet 2

Inventory Software

Operating system software description(s):
Application software description(s):

CHAPTER 3

DETERMINE DATA SENSITIVITY

Data sensitivity is determined within the methodology by completing Worksheet 3, which consists of the steps described in the paragraphs below.

DOCUMENT THE INFORMATION FLOW

Document the information flow in the business process that is or will be aided by using the EDI system. This should be done by listing the transaction set used (if that information is available) and describing the type of action that occurs when each type of EDI transaction is sent. Note that the same transaction set is sometimes used for several different types of actions; each of those actions should be listed on the worksheet.

DEFINE THE TYPE OF SENSITIVE DATA

For each type of action used, determine whether the data that are or will be processed are sensitive. The various types of unclassified/sensitive data are shown in Table 1 and footnote "a" of Worksheet 3 . If the data are not sensitive and could be viewed by anyone under any circumstances, enter a zero in Worksheet 3's "Types of sensitive/unclassified data" column. Otherwise, enter the number of the type of sensitive/unclassified data used in the convention in the "Types of sensitive/ unclassified data" column. An example of a completed Worksheet 3 is shown in Table 2.

The purpose of determining the types of sensitive data that are processed is to assist with selecting appropriate protection mechanisms for the data on the basis of security requirements already provided by statute or agency determination. Information required to be protected under statute includes privacy information (protected under the Privacy Act), financial information (protected under the Federal Managers' Financial Integrity Act), taxpayer information, and individual census data. Agency determinations for security requirements are in use for designations such as "For Official Use Only." In its November 1992 Computer Systems Laboratory (CSL) Bulletin entitled "Sensitivity of Information," NIST states that all

nontrivial Government information requires some level of protection at least at one of the three dimensions of confidentiality, integrity, and availability. Thus, even if the information processed on an EDI system is not sensitive, it still requires some kind of security protection.

TABLE 1

TYPES AND EXAMPLES OF UNCLASSIFIED/SENSITIVE DATA

Number	Type	Examples
0	Not sensitive	• Requests for proposals or requests for bids • Announcements of or minutes from meetings open to the public
1	*Vital records*: Records essential for maintaining continuity of Government activities during a national emergency	• Emergency operations records ▸ General management records ▸ Emergency mission records • Rights and interests records ▸ Legal rights records ▸ Fiscal records
2	*Privacy Act information*: Records maintained on an individual that contain a name, identifying number or symbol, or particulars assigned to an individual	• Payment and retirement benefits records • Medical and psychological records • Educational achievement records
3	*Official use only*: Unclassified information that may be exempt from public release under the Freedom of Information Act	• Internal correspondence • Working papers
4	*National security related (but unclassified)*: Unclassified information that alone or in the aggregate reveals information regarding a "high-value" U.S. program or initiative	• International traffic-in-arms control • Unclassified intelligence information • Controlled scientific and technical information • Foreign exchange information
5	*Security management related*: Unclassified information developed and stored to administer and ensure compliance with security programs	• Limited access information • Security/internal audit information • Legal information • Other audit information
6	*Proprietary information*: Unclassified business information the release of which could provide unfair advantage to business competitors	• Cost/pricing information

Source: Adapted from the *U.S. Department of Energy (DOE) Risk Assessment Methodology, Volumes I and II*, issued by the U.S. Department of Commerce, National Technical Information Service, May 1990, p. 39.

Worksheet 3

Sensitivity of EDI Data

Item number	Transaction set (if known)	Type of action	Types of sensitive/ unclassified data[a]	Comments
1				
2				
3				
4				
5				

[a]Types of unclassified/sensitive data (see Table 1 for definitions of these terms):

0 – Not sensitive
1 – Vital records
2 – Privacy Act information
3 – Official use only
4 – National security related (but unclassified)
5 – Security management related
6 – Proprietary information

TABLE 2

EXAMPLE OF A COMPLETED
WORKSHEET 3, SENSITIVITY OF EDI DATA

Item number	Transaction set (if known)	Type of action	Types of sensitive/ unclassified data[a]	Comments
1	810	Submit invoice information	1	
2	810	Submit progress payment information	1	
3	810	Submit public voucher information	1, 6	
4	824	Receive an acceptance/rejection notice of an electronic invoice or progress payment (*Applications Advice*)	1, 6	
5	997	Receive an acceptance/ rejection notice of an electronic invoice (*Functional Acknowledgment*)	0	

[a]Types of unclassified/sensitive data (see Table 1 for definitions of these terms):

0 – Not sensitive
1 – Vital records
2 – Privacy Act information
3 – Official use only
4 – National security related (but unclassified)
5 – Security management related
6 – Proprietary information

CHAPTER 4

REVIEW THREATS AND IDENTIFY INFORMATION SECURITY REQUIREMENTS

OVERVIEW

The primary threats to an EDI application system and its data are the following:

- Unauthorized disclosure of data
- Unauthorized modification of data
- Sender repudiation of transactions
- Receiver repudiation of transactions
- Unauthorized system access
- Lack of system availability.

The several sections of Worksheet 4 comprise an EDI information security controls questionnaire that must be completed in order to assess the vulnerabilities that exist within the EDI system being examined.

Worksheets 4.1 and 4.2 list information security controls that should be used within EDI systems. Worksheet 4.1 addresses EDI *system-wide* information security requirements and should be completed only once. Because Worksheet 4.2 addresses *action-specific* information security requirements, a copy of Worksheet 4.2 should be made and then completed for *each* type of action you listed in Worksheet 3 that involves the transfer of sensitive/unclassified information.

GENERAL INSTRUCTIONS FOR WORKSHEETS 4.1 AND 4.2

Answer each question by checking either "Yes" or "No." A "No" answer indicates that a security vulnerability is present in that area. Control procedures for each item on Worksheet 4.1 should be described in the space provided below each group of items. When providing descriptions of procedures used within each area, reference each control item by number and list the procedures in order from the least

rigorous to the most rigorous. Space for describing control procedures for the items on Worksheet 4.2 is provided beneath each group of items.

System-Wide Information Security Requirements

Authentication and Nonrepudiation

Authentication is the establishment of the validity of the identity of the message's originator.

The following are examples of techniques used for authentication:

- Including certain reference numbers or passwords known only to the sender and receiver within the body of a message (imbedded references)
- Sending an acknowledgment for each transaction without repeating the transaction's contents (functional acknowledgement)
- Sending an acknowledgement that repeats back messages or parts of messages (message repetition acknowledgment)
- Using a trusted third party to provide security services such as status reports that document when and to whom transactions were sent and received
- Using access control techniques such as passwords or smart cards
- Using cryptographic techniques such as message authentication codes and digital signatures.

Protecting against *nonrepudiation* involves ensuring that one of the two parties to a data interchange cannot falsely deny involvement due to proof that can be offered to a third party. The techniques listed above for authentication also provide protection against nonrepudiation. Two evolving techniques that provide a strong level of protection against nonrepudiation are third-party notarization and the use of public key cryptography.

If an access control mechanism is in place to control access to the EDI application, then procedures should exist for adding and deleting users to the application and for associating them with each other.

Written agreements between EDI trading partners should exist that provide guidance concerning the people who can be allowed user access to the EDI system, the

users' assigned level of access, and the user interactions and data standards that are allowed.

Contingency Planning and Backup and Recovery

The availability of a system and its data are assured through the use of contingency planning and data backup and recovery procedures. For example, archived data are often used for backup and recovery purposes.

Electronic Records Management

According to guidance provided by the National Archives and Records Administration (NARA) on the management of electronic records in the Code of Federal Regulations, 36 CFR Part 1234, "Electronic records may be admitted in evidence to Federal courts for use in court proceedings [Federal Rules of Evidence 803(8)] if trustworthiness is established by thoroughly documenting the recordkeeping system's operation and the controls imposed upon it." Documentation about a system's use can be obtained by using electronic audit trails. Information provided by a trusted third party's status report should be included in the audit trail information. Documentation about the controls imposed upon a system can be obtained by performing internal controls reviews on a regular basis. Within the DoD, internal controls reviews of systems are usually conducted as part of an organization's Internal Management Control Program (IMCP) as described in Administrative Instruction Number 90 issued by the Secretary of Defense on 8 November 1988. The legal basis for the IMCP is the Federal Managers' Financial Integrity Act (FMFIA) of 1982.

Action-Specific Information Security Requirements

Message Integrity

Message integrity is protected by ensuring that messages are changed only in a specified and authorized manner.

Examples of techniques used to ensure message integrity are as follows:

- Including a unique identification code with each transaction to distinguish it from all others (imbedded references)
- Sending an acknowledgment that repeats back messages or parts of messages (message repetition acknowledgment)
- Recalculating and verifying hash totals (internal message verification)
- Using cryptographic techniques such as "message authentication codes" or digital signatures.

Data Confidentiality

Data Confidentiality is protected by preventing sensitive information from being disclosed to unauthorized recipients.

The following are examples of techniques used to ensure data confidentiality:

- Using access control mechanisms such as passwords or smart cards
- Using cryptographic techniques, such as use of the Data Encryption Standard (DES).

Worksheet 4.1

System-Wide Information Security Requirements

Item	Controls	Yes[a]	No
4.1.1 Authentication and Nonrepudiation			
1.	Do written agreements between EDI trading partners exist?		
2.	Are any authentication and nonrepudiation mechanisms (e.g., imbedded references, functional acknowledgments, message repetition acknowledgments, access control techniques, message authentication codes, or digital signatures) in use within the EDI system? If an access control mechanism is not used, skip questions 3 through 5 below.		
3.	If different levels of access are available on the system (e.g. some users can access only certain types of transactions), describe how such access levels are assigned and enforced.		
4.	Do procedures exist for adding and deleting users' access to the EDI application system?		
5.	If passwords are used, answer 5.a through 5.c below:		
5.a	Does each user have a unique user identification code (ID) and password that is not shared with others?		
5.b	Are passwords required to be at least five characters long?		
5.c	Are passwords required to be changed at least once every 6 months?		
Item	Use this space to describe control procedures (attach additional sheets if necessary).		

[a] If yes, describe control procedures below.

Worksheet 4.1

System-Wide Information Security Requirements (Continued)

Item	Controls	Yes[a]	No
4.1.2 Contingency Planning and Backup and Recovery			
6.	Does a comprehensive contingency plan exist that documents procedures to use in case the EDI system is unavailable?		
	If Yes, is the plan tested at least annually?		
7.	Are backups of software and data made on a regular basis?		
	If Yes, is off-site storage used for backups?		
8.	Do recovery procedures exist?		
	If Yes, are recovery procedures tested regularly?		
Item	Use this space to describe control procedures (attach additional sheets if necessary).		

[a] If yes, describe control procedures below.

Worksheet 4.1

System-Wide Information Security Requirements (Continued)

Item	Controls	Yes[a]	No
4.1.3 Electronic Records Management			
9.	Does the EDI system have an electronic audit trail? If not, skip questions 10 through 13.		
10.	Does the audit trail record information about all events that occur? (List below the types of events that are recorded in the audit trail, e.g., modifications to EDI transactions, data entry, EDI and transaction receipt, and translation, etc.)		
11.	Does the audit trail record the following information for each event:		
11.a	Type of event?		
11.b	Date?		
11.c	Time?		
11.d	User ID(s) involved?		
Item	Use this space to describe control procedures (attach additional sheets if necessary).		

[a] If yes, describe control procedures below.

Worksheet 4.1

System-Wide Information Security Requirements (Continued)

Item	Controls	Yes[a]	No
4.1.3 Electronic Records Management (continued)			
12.	Is the audit trail protected from unauthorized access (e.g., by individuals outside information security management)?		
13.	Is the audit trail monitored on a regular basis to ensure that unauthorized activities are not occurring?		
14.	Are complete copies of each transmitted EDI message stored in an audit trail or archived elsewhere?		
15.	Are periodic internal controls reviews or audits performed for the EDI system?		
Item	Use this space to describe control procedures (attach additional sheets if necessary).		

[a] If yes, describe control procedures below.

Worksheet 4.2

Action-Specific Information Security Requirements

Item	Controls	Yes	No
4.2.1 Message Integrity			
Type of action (from Worksheet 3):			
1.	Are any mechanisms that ensure message integrity (e.g., imbedded references, message repetition acknowledgment, internal message verification, and message authentication codes or digital signatures) in use within the EDI system?		
	If yes, describe procedures used.		
4.2.2 Data Confidentiality			
2.	Are any mechanisms that ensure data confidentiality (e.g., access control mechanisms, cryptographic techniques) in use within the EDI system?		
	If yes, describe procedures used.		

Note: A copy of this page should be made and then completed for each type of action listed in Worksheet 3.

CHAPTER 5

SELECT PROTECTIVE COUNTERMEASURES

Worksheets 5.1 and 5.2 document the risk profile for each security area and determine the protective countermeasures that should be implemented. Worksheet 5.1 addresses EDI system-wide countermeasures and should be completed only once; however, because Worksheet 5.2 addresses action-specific countermeasures, a copy of Worksheet 5.2 should be made and then completed for each type of action listed in Worksheet 3.

To complete Worksheets 5.1 and 5.2, refer back to the completed Worksheets 4.1 and 4.2 and then do the following:

1. For each security area listed on Worksheets 5.1 and 5.2, turn to the corresponding (completed) section within Worksheets 4.1 and 4.2.

2. For each security area, list the vulnerabilities in the "Vulnerabilities" columns of Worksheets 5.1 and 5.2. Vulnerabilities can be found by referring back to the corresponding security area within Worksheets 4.1 and 4.2 and noting the questions that were answered "No." Any "No" answers on Worksheets 4.1 and 4.2 denote vulnerabilities for that security area.

3. For each of the security vulnerabilities that you list in the "Vulnerabilities" column of Worksheet 5.1, the annual loss exposure that would occur if the vulnerability was exploited should be calculated and entered in the "Annual loss exposures" columns of Worksheets 5.1 and 5.2. The following method for calculating annual loss exposures is taken from Federal Information Processing Standards (FIPS) Publication 65, "Guideline for Automatic Data Processing Risk Analysis" dated 1 August 1979, by the U.S. Department of Commerce. Annual loss exposure is calculated by obtaining the product of the estimated impact of an event and its estimated frequency of occurrence. The time needed to estimate impact and frequency of occurrence is reduced considerably by using orders of magnitude as shown in Table 3. Those figures are combined in Table 4 to illustrate annual loss exposure values.

TABLE 3

ORDERS OF MAGNITUDE OF ESTIMATED IMPACT AND FREQUENCY

Impact (i): values of i ($)		Frequency (f): values of f	
1	$10	1	Once in 300 years
2	100	2	Once in 30 years
3	1,000	3	Once in 3 years
4	10,000	4	Once in 100 days
5	100,000	5	Once in 10 days
6	1,000,000	6	Once per day
7	10,000,000	7	10 times per day
8	100,000,000	8	100 times per day

TABLE 4

COMBINED MATRIX OF IMPACT, FREQUENCY, AND ANNUAL LOSS EXPOSURE

		Once in 300 yrs. (≃ 100,000 days) ($)	Once in 30 yrs. (≃ 10,000 days) ($)	Once in 3 yrs. (≃ 1,000 days) ($)	Once in 100 days ($)	Once in 10 days ($)	Once per day ($)	10 times per day ($)	100 times per day ($)
$	f = / i =	1	2	3	4	5	6	7	8
10	1					$300	$3,000		$300k
100	2				$300	3,000	30k	$300k	3M
1,000	3			$300	3,000	30k	300k	3M	30M
10,000	4		$300	3,000	30k	300k	3M	30M	
100,000	5	$300	3,000	30k	300k	3M	30M	300M	
1,000,000	6	3,000	30k	300k	3M	30M	300M		
10,000,000	7	30k	300k	3M	30M	300M			
100,000,000	8	300k	3M	30M	300M				

Notes: k = thousands of dollars; M = millions of dollars; ≃ = approximately.

In determining annual loss exposures for each security vulnerability, remember to include in the estimate the monetary cost of the following activities that may result from someone taking advantage of the vulnerability:

- Investigations
- Adverse publicity
- Litigation
- Staff disciplinary action (e.g., employee reprimand, dismissal, and hiring and training a new employee)
- Any downtime; delay; interim operation; or repair, recovery, and/or replacement of hardware, software, and/or data
- Future business or funding losses
- Fraud or embezzlement.

4. For those security areas having unacceptable current risk profiles, indicate the countermeasures that should be implemented. If (1) your data are highly sensitive and/or (2) the impact upon your organization if your system is unavailable is medium, high, or very high (see Worksheet 1), consider implementing protection techniques that provide a medium or higher level of protection. Remember that when examples of techniques within each area are given in Chapter 4, techniques that provide the least protection are listed first, and techniques that provide the most protection are listed last. Consult an information systems security professional for further guidance about the protection techniques that will best meet your needs.

5. As you examine available security mechanisms to use as countermeasures, determine the approximate costs for implementing the countermeasures and enter those estimated costs in the "Estimated costs of security mechanisms" columns of Worksheets 5.1 and 5.2. The estimates may be approximate dollar amounts for products and/or may reflect the approximate amount of labor time that would be required to implement products or security procedures. Refer to security product literature to determine the approximate costs for acquiring and implementing different products. The maximum acceptable cost of any countermeasure should be limited by the size of the annual loss exposure that would be mitigated by the countermeasure. For example, if the total estimated cost for recovering a critical data base is $10,000, an approximate expense of less than $10,000 to back up the data base would be justified.

Worksheet 5.1

Countermeasures Identification
System-Wide Information Security Requirements

Security area	Vulnerabilities	Annual loss exposures	Security mechanisms to be implemented	Estimated costs of security mechanisms
Authentication and nonrepudiation (4.1.1)				
Contingency planning and backup and recovery (4.1.2)				
Electronic records management (4.1.3)				

Worksheet 5.2

Countermeasures Identification
Action-Specific Information Security Requirements

Type of action (from Worksheet 4):				
Security area	**Vulnerabilities**	**Annual loss exposures**	**Security mechanisms to be implemented**	**Estimated costs of security mechanisms**
Message integrity (4.2.1)				
Data confidentiality (4.2.2)				

Note: A copy of this page should be made and then completed for each type of action listed in Worksheet 4.

GLOSSARY

ASC X12	=	Accredited Standards Committee X12
CFR	=	Code of Federal Regulations
CSL	=	Computer Systems Laboratory
DES	=	Data Encryption Standard
DoDD	=	Department of Defense Directive
DOE	=	Department of Energy
EC	=	Electronic Commerce
EDI	=	electronic data interchange
FIPS	=	Federal Information Processing Standard
FMFIA	=	Federal Managers' Financial Integrity Act
IMCP	=	Internal Management Control Program
NARA	=	National Archives and Records Administration
NIST	=	National Institute of Standards and Technology

REPORT DOCUMENTATION PAGE

Form Approved
OPM No. 0704-0188

1. AGENCY USE ONLY *(Leave Blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	May 1993	Final

4. TITLE AND SUBTITLE
Risk Assessment Methodology for EDI Unclassified/Sensitive Information Systems

5. FUNDING NUMBERS
C MDA903-90-C-0006
PE 0902198D

6. AUTHOR(S)
Julie A. Smith

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Logistics Management Institute
6400 Goldsboro Road
Bethesda, MD 20817-5886

8. PERFORMING ORGANIZATION REPORT NUMBER
LMI-DL203R3

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Robert M. Harrison
Defense Information Technology Services Organization
Defense Information Systems Agency
Room 3A590, Cameron Station
Alexandria, VA 22304

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION/AVAILABILITY STATEMENT
A: Approved for public release; distribution unlimited

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

Because it is not cost-effective to implement more security procedures than a particular environment requires, defining security requirements based on the results of a thorough risk analysis provides an effective way to control the cost of security for information systems. The steps involved in the EDI risk assessment methodology presented in this paper are the same basic steps found in most types of risk assessment: define assets, review threats, identify security requirements, and select protective countermeasures. The methodology addresses all of the primary threats to an EDI application system and its data, which include the following: unauthorized disclosure of data, unauthorized modification of data, sender repudiation of transactions, receiver repudiation of transactions, unauthorized system access, and lack of system availability.

14. SUBJECT TERMS
Information systems, electronic data interchange (EDI), Security, Risk Assessment

15. NUMBER OF PAGES
35

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL